

Contract Name:
Contract Number:

BUSINESS ASSOCIATE AGREEMENT With Contract

This Business Associate Agreement is incorporated into the Underlying Contract known as _____ and is made between the Wisconsin Department of Health Services, _____ (“Covered Entity”) and the _____ (“Business Associate”), collectively the “Parties.”

This Agreement is specific to those services, activities, or functions performed by the Business Associate on behalf of the Covered Entity when such services, activities, or functions are covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) including all pertinent regulations (45 CFR Parts 160 and 164) issued by the U.S. Department of Health and Human Services. Services, activities, or functions covered by this Agreement include, but are not limited to:

The Covered Entity and Business Associate agree to modify the Contract to incorporate the terms of this Agreement and to comply with the requirements of HIPAA addressing confidentiality, security and the transmission of individually identifiable health information created, used or maintained by the Business Associate during the performance of the Contract and after Contract termination. The parties agree that any conflict between provisions of the Contract and the Agreement will be governed by the terms of the Agreement.

1. DEFINITIONS

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information and Use.

Specific definitions:

- a. Business Associate: “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].
- b. Covered Entity: “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103 and in reference to the party in this agreement shall mean the Wisconsin Department of Health Services.
- c. HIPAA Rules: “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

2. RESPONSIBILITIES OF BUSINESS ASSOCIATE

- a. Business Associate shall not use or disclose any PHI except as permitted or required by the Contract or this Agreement, as permitted or required by law, or as otherwise authorized in writing by the Covered Entity, if done by the Covered Entity. Unless otherwise limited herein, Business Associate may use or disclose PHI for Business Associate’s proper management and administrative services, to carry out legal responsibilities of Business Associate, and to provide data aggregation services relating to health care operations of the Covered Entity if required under the Agreement.
- b. Business Associate shall not request, use or disclose more than the minimum amount of PHI necessary to accomplish the purpose of the use or disclosure.
- c. Business associate shall inform the Covered Entity if it or its subcontractors will perform any work outside United States America that involves access to, or the disclosure of PHI.

3. SAFEGUARDING AND SECURITY OF PROTECTED HEALTH INFORMATION

- a. Business Associate shall use appropriate safeguards, including complying with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement.
- b. Business Associate shall cooperate in good faith in response to any reasonable requests from the Covered Entity to discuss, review, inspect, and/or audit Business Associate's safeguards.

4. REPORTING OF A VIOLATION TO COVERED ENTITY BY BUSINESS ASSOCIATE

The Business Associate shall report to Covered Entity any use or disclosure of PHI not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410 and any security incident.

- a. **Discovery of a Violation.** The Business Associate must inform the Covered Entity by telephone call, plus email or fax within the next business day following the discovery of any violation,
 - (i) The Violation shall be treated as "discovered" as of the first day on which the Violation is known to the Business Associate, or, by exercising reasonable diligence would have been known to the Business Associate.
 - (ii) Notification shall be provided to one of the contact persons as listed in section d.
 - (iii) Notification shall occur within the first business day that follows discovery of the Violation.
- b. **Mitigation.** The Business Associate shall take immediate steps to mitigate any harmful effects of the unauthorized use, disclosure, or loss. The Business Associate shall reasonably cooperate with the Covered Entity's efforts to seek appropriate injunctive relief or otherwise prevent or curtail such threatened or actual breach, or to recover its PHI including complying with a reasonable Corrective Action Plan.
- c. **Investigation of Breach.** The Business Associate shall immediately investigate the Violation and report in writing within one week, to a contact listed in section 5d with the following information:
 - (i) Each Individual who's PHI has been or is reasonably to have been accessed, acquired, or disclosed during the Incident,
 - (ii) A description of the types of PHI that were involved in the Violation (such as full name, social security number, date of birth home address, account number and etc.).
 - (iii) A description of unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data,
 - (iv) A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized,
 - (v) A description of probable causes of the improper use or disclosure,
 - (vi) A brief description of what the Business Associate is doing to investigate the Incident, to mitigate losses and to protect against further Violations,
 - (vii) The actions the Business Associate has undertaken or will undertake to mitigate any harmful effect of the occurrence, and
 - (viii) A corrective action plan that includes the steps the Business Associate has taken or shall take to prevent future similar Violations.
- d. **Covered Entity Contact Information.** To direct communications to above referenced Covered Entity's staff, the Business Associate shall initiate contact as indicated herein. The Covered Entity reserves the right to make changes to the contact information by giving written notice to the Business Associate.

Covered Entity Program Manager:	DHS Privacy Officer	DHS Security Officer
Name	c/o Office of Legal Counsel	Department of Health Services
Address	Department of Health Services	1 W. Wilson St.
	1 W. Wilson St.	Madison, WI 53707
Phone	Madison, WI 53707	608-261-8310
Email	608-266-5484	

5. USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION BY SUBCONTRACTORS OF THE BUSINESS ASSOCIATE

In accordance with 45 CFR 164.502(e)(1) and 164.308(b) , if applicable, the Business Associate shall ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business

Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information.

6. COMPLIANCE WITH ELECTRONIC TRANSACTIONS AND CODE SET STANDARDS

If the Business Associate conducts any Standard Transaction for, or on behalf, of a Covered Entity, the Business Associate shall comply, and shall require any subcontractor or agent conducting such Standard Transaction to comply, with each applicable requirement of Title 45, Part 162 of the Code of Federal Regulation. The Business Associate shall not enter into, or permit its subcontractors or agents to enter into, any Agreement in connection with the conduct of Standard Transactions for or on behalf of Covered Entity that:

- a. Changes the definition, Health Information condition, or use of a Health Information element or segment in a Standard;
- b. Adds any Health Information elements or segments to the maximum defined Health Information Set;
- c. Uses any code or Health Information elements that are either marked "not used" in the Standard's Implementation Specification(s) or are not in the Standard's Implementation Specifications(s);
- d. Changes the meaning or intent of the Standard's Implementations Specification(s).

7. ACCESS TO PROTECTED HEALTH INFORMATION

At the direction of the Covered Entity, the Business Associate agrees to provide access, in accordance with 45 CFR 164.524, to any PHI held by the Business Associate, which Covered Entity has determined to be part of Covered Entity's Designated Record Set, in the time and manner designated by the Covered Entity. This access will be provided to Covered Entity or, as directed by Covered Entity, to an Individual, in order to meet requirements under the Privacy Rule.

8. AMENDMENT OR CORRECTION TO PROTECTED HEALTH INFORMATION

At the direction of the Covered Entity, the Business Associate agrees to amend or correct PHI held by the Business Associate which the Covered Entity has determined is part of the Covered Entity's Designated Record Set, in the time and manner designated by the Covered Entity in accordance with 45 CFR 164.526.

9. DOCUMENTATION OF DISCLOSURES OF PROTECTED HEALTH INFORMATION BY THE BUSINESS ASSOCIATE

The Business Associate agrees to document and make available to the Covered Entity or (at the direction of the Covered Entity) to an Individual such disclosures of PHI to respond to a proper request by the Individual for an accounting of disclosures of PHI, in accordance with 45 CFR 164.528.

10. INTERNAL PRACTICES

The Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI available to the Covered Entity, or to the federal Secretary of Health and Human Services (HHS) in a time and manner determined by the Covered Entity or the HHS Secretary or designee, for purposes of determining compliance with the requirements of HIPAA.

11. TERM AND TERMINATION OF AGREEMENT

- a. The Business Associate agrees that if in good faith the Covered Entity determines that the Business Associate has materially breached any of its obligations under this Agreement, the Covered Entity may:
 - (i) Exercise any of its rights to reports, access and inspection under this Agreement;
 - (ii) Require the Business Associate within a 30 day period to cure the breach or end the violation;
 - (iii) Terminate this Agreement if the Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity;
 - (iv) Immediately terminate this Agreement if the Business Associate has breached a material term of this Agreement and cure is not possible.
- b. Before exercising either (ii) or (iii), the Covered Entity will provide written notice of preliminary determination to the Business Associate describing the violation and the action the Covered Entity intends to take.

12. RETURN OR DESTRUCTION OF PROTECTED HEALTH INFORMATION

Upon termination, cancellation, expiration or other conclusion of this Agreement, the Business Associate will:

- a. Return to the Covered Entity or, if return is not feasible, destroy all PHI and any compilation of PHI in any media or form. The Business Associate agrees to ensure that this provision also applies to PHI of the Covered Entity in possession of subcontractors and agents of the Business Associate. The Business Associate agrees that any original record or copy of PHI in any media is included in and covered by this provision, as well as all original or copies of PHI provided to subcontractors or agents of the Business Associate. The Business Associate agrees to complete the return or destruction as promptly as possible, but not more than **thirty (30)** business days after the conclusion of this Agreement. The Business Associate will provide written documentation evidencing that return or destruction of all PHI has been completed.
- b. If the Business Associate destroys PHI, it shall be done with the use of technology or methodology that renders the PHI unusable, unreadable, or undecipherable to unauthorized individuals as specified by HHS in HHS guidance. Acceptable methods for destroying PHI include:
 - (i) For paper, film, or other hard copy media: shredded or destroyed in order that PHI cannot be read or reconstructed; and
 - (ii) For electronic media: cleared, purged or destroyed consistent with the standards of the National Institute of Standards and Technology (NIST).

Redaction is specifically excluded as a method of destruction of PHI, unless the information is properly redacted so as to be fully de-identified.

- c. If the Business Associate believes that the return or destruction of PHI is not feasible, the Business Associate shall provide written notification of the conditions that make return or destruction not feasible. If the Business Associate and Covered Entity agree that return or destruction of PHI is not feasible, the Business Associate shall extend the protections of this Agreement to PHI and prohibit further uses or disclosures of the PHI of the Covered Entity without the express written authorization of the Covered Entity. Subsequent use or disclosure of any PHI subject to this provision will be limited to the use or disclosure that makes return or destruction not feasible.

13. COMPLIANCE WITH STATE LAW

The Business Associate acknowledges that PHI from the Covered Entity may be subject to state confidentiality laws. Business Associate shall comply with the more restrictive protection requirements between state and federal law for the protection of PHI.

14. MISCELLANEOUS PROVISIONS

- a. Indemnification for Breach. Business Associate shall to the extent allowed by Wisconsin law, indemnify the Covered Entity for costs associated with any Incident involving the acquisition, access, use or disclosure of PHI in a manner not permitted under HIPAA Rules.
- b. Automatic Amendment. This Agreement shall automatically incorporate any change or modification of applicable state or federal law as of the effective date of the change or modification. The Business Associate agrees to maintain compliance with all changes or modifications to applicable state or federal law.
- c. Interpretation of Terms or Conditions of Agreement. Any ambiguity in this Agreement shall be construed and resolved in favor of a meaning that permits the Covered Entity and Business Associate to comply with applicable state and federal law.
- d. Survival. All terms of this Agreement that by their language or nature would survive the termination or other conclusion of this Agreement shall survive.

IN WITNESS WHEREOF, the undersigned have caused this Agreement to be duly executed by their respective representatives.

COVERED ENTITY

BUSINESS ASSOCIATE

Print Name: _____ Print Name: _____

SIGNATURE: _____ **SIGNATURE:** _____

Title: _____ Title: _____

Date: _____ Date: _____